Diagnóstico LGPD

1. [Capacitação Interna] – Todos os colaboradores da sua organização conhecem os conceitos da LGPD, seus impactos no negócio e os cuidados que devem ser observados?

2. [Capacitação Interna] – A organização mantém de forma estruturada, faz a disseminação e tem o objetivo de engajar todos os colaboradores sobre a importância da proteção de dados pessoais?

3. [Consentimento e Coleta Dados Pessoais] – Toda a coleta de dados pessoais que sua organização faz, permite que o seu titular expresse o livre consentimento par tal ação?

4. [Contratos] – Os modelos de contratos da sua organização, sejam eles clientes, fornecedores, terceiros ou colaboradores estão adequados a LGPD?

5. [Contratos] – Os contratos com todas as partes sempre incluem a causa, motivo, ação e duração do tratamento de dados?

6. [Direito do Titular de Dados] – O titular de dados pessoais que a sua organização administra possui todos os direitos de acesso, correção, revisão e portabilidade que a LGPD exige?

7. [DPO] – A organização possui um encarregado de dados/DPO (Data Protection Officer) nomeado e com seus dados públicos aos titulares de dados?

8. [Políticas de Segurança de Informação] – Sua organização já possui uma política de segurança e privacidade de dados pessoais identificando como coletar e com quem compartilhar?

9. [Privacy by Design] – Sua empresa já utiliza na construção ou contratação de aplicações e soluções tecnológicas o critério “Privacy by Design” como mais uma garantia de adequação a LGPD?

10. [Violação e Retenção de Dados Pessoais] – Para todos os dados pessoais coletados pela sua organização, há políticas claras de retenção, armazenamento e comunicação em caso de violação?

11. [Aplicação Técnicas de Segurança] – Sua empresa possui nível adequado de proteção tecnológico no que tange a segurança da informação incluindo antivírus, firewall, backup periódico, acessos remotos por VPN segura, registros de logs de uso, sistemas

digitais conseguem classificar acesso a dados pessoais e dados sensíveis e criptografia sobre as bases de dados?

12. [Governança] – Consideramos as questões relacionadas à proteção de dados como parte do projeto e implementação de sistemas, serviços, produtos e práticas comerciais?

13. [Governança] – A organização sempre aplica o RIPD (Relatório de Impacto de Proteção de Dados) quando realizamos tomadas de decisões automatizadas que envolvam as pessoas ou produtos?

14. [Governança] – A organização realiza revisões periódicas e documentadas sobre o tratamento de dados pessoais que realiza?

15. [Jurídico] – A forma que a organização trata os dados pessoais dos titulares está sempre classificada em uma das bases legais de acordo com a LGPD?

16. [Jurídico] – A organização possui um mapeamento das fontes de entradas de dados, sejam elas, física e/ou digital?

17. [Jurídico] – A organização entende claramente a responsabilidade de proteger os dados dos titulares de dados e as consequências em caso de incidente de vazamentos de dados pessoais?

18. [Marketing] – A organização considera o consentimento fornecido pelo usuário antes de oferecer campanhas publicitárias ou similares?

19. [Processos] – A organização possui um mapeamento das fontes de entrada, coleta, uso, bloqueio e demais tratamento de dados pessoais documentado e atualizado?

20. [Processos] – A organização possui uma matriz e análise de riscos dos processos identificando e priorizando de forma estruturada os planos de ação sobre a proteção de dados pessoais?